Nagios

cooler than it looks

Outline

- sysadmin 101
- Nagios Overview
- Installing nagios
- NRPE / NSCA
- Other Stuff
- Questions

Sysadmin 101

- Every sysadmin needs a decent toolkit...

Sysadmin 101

- Every sysadmin needs a decent toolkit...
- Ticketing / issue tracking / helpdesk

Sysadmin 101

- Every sysadmin needs a decent toolkit...
- Ticketing / issue tracking / helpdesk
- Trend monitoring

Sysadmin 101

- Every sysadmin needs a decent toolkit...
- Ticketing / issue tracking / helpdesk
- Trend monitoring
- Outage / warning alarms

Sysadmin 101

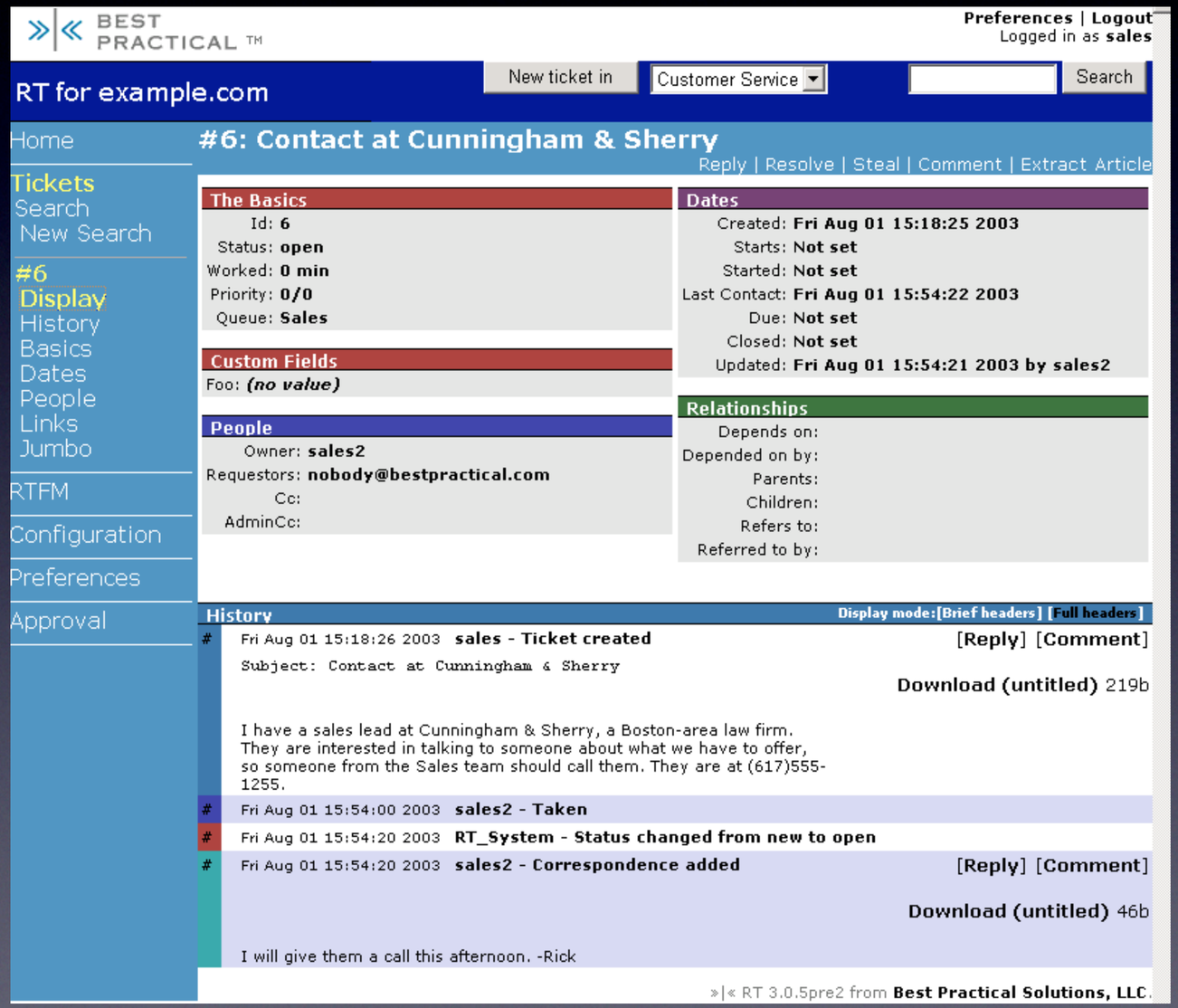
- Every sysadmin needs a decent toolkit...
- Ticketing / issue tracking / helpdesk
- Trend monitoring
- Outage / warning alarms
- Espresso Maker

Ticketing system

- Prevents mailbox overload
- see Limoncelli ‘Time Management for System Administrators’ - Glorified TODO list
- Highlights recurring themes
- Users like the feedback

Example ticketing systems

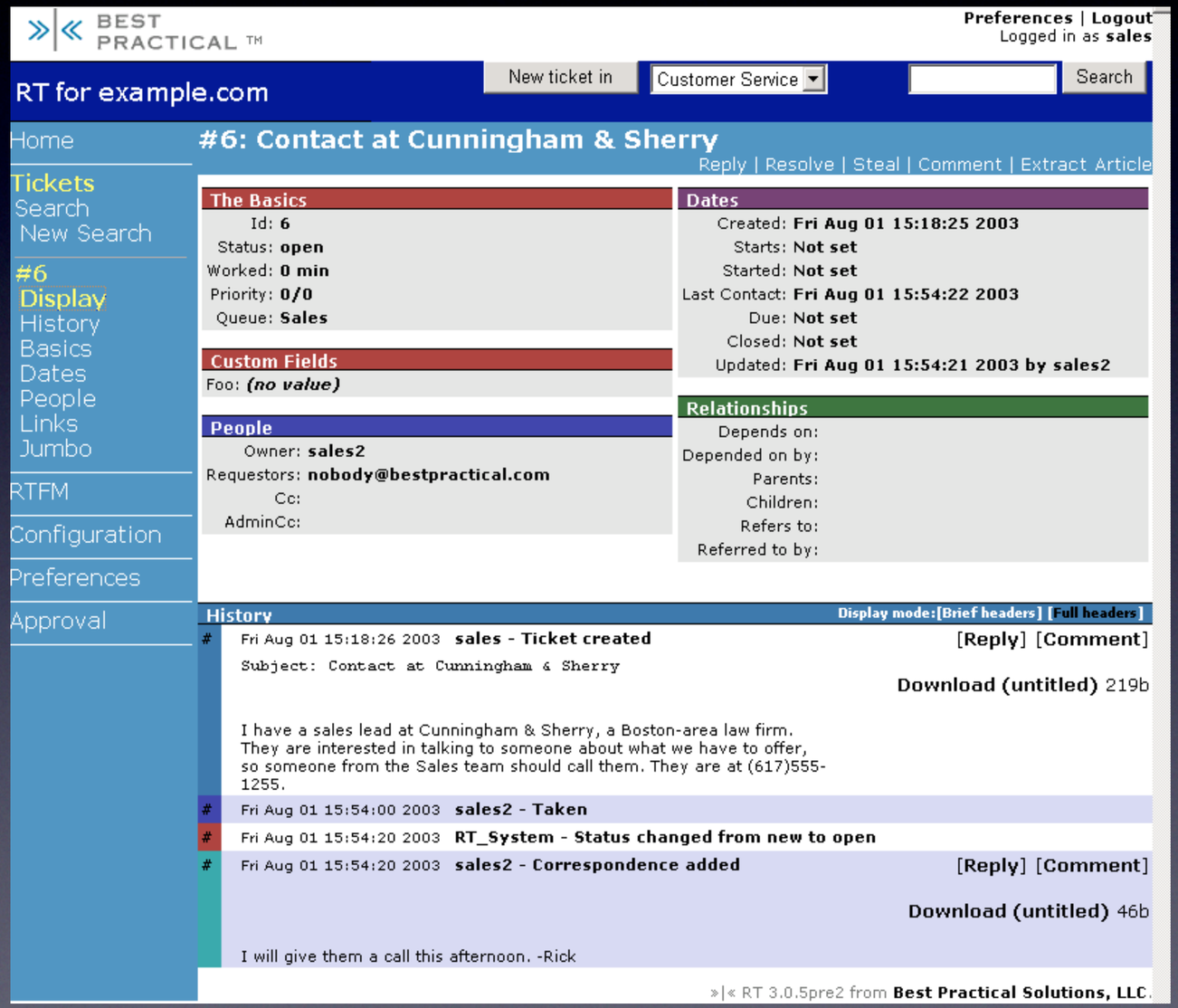
- Remedy / BMC
- Footprints
- GGUS
- Request Tracker



Example ticketing systems

- Remedy / BMC
- Footprints
- GGUS
- Request Tracker

Fix before users notice?

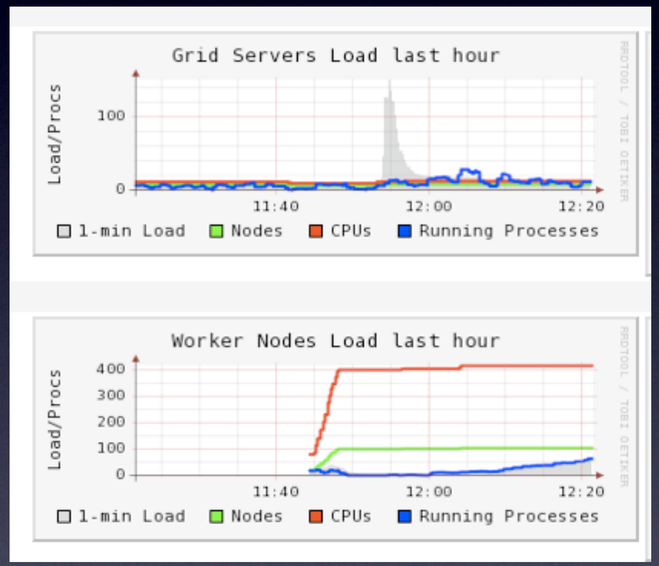


Trend Monitoring

- X disk free - is that up or down?
- Temperature - What's normal?
- Network activity - have you been slashdotted?

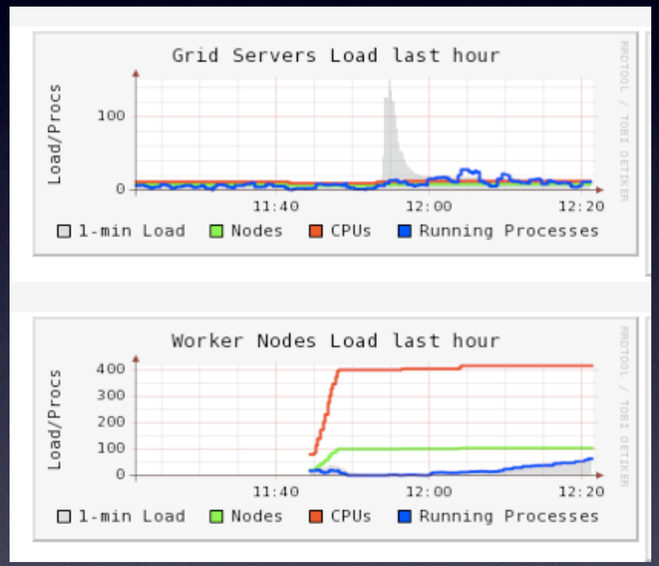
Ganglia

- Most cluster vendors package it.
- http://ganglia.sf.net



Ganglia

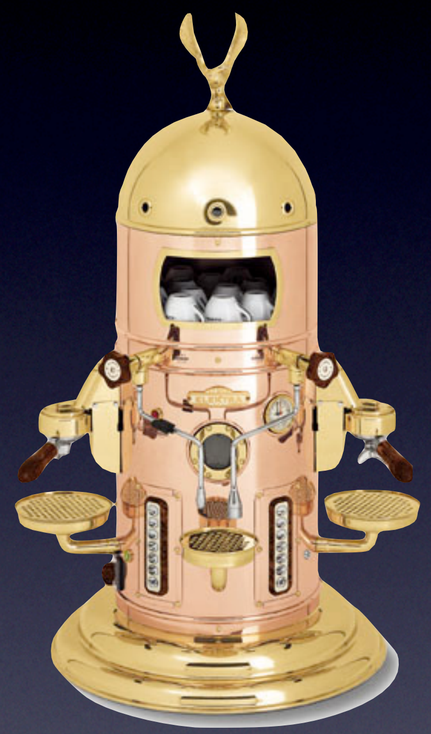
- Most cluster vendors package it.
- http://ganglia.sf.net
- Can be fed from MonAMI...



‘Something Broke’

- Various companies sell products that can monitor boxes / network / programs
  - eg, Tivoli, NetView
  - Nagios may not be ‘The Best’ - but it’s free, good enough and contributed to by the HEP community.

Espresso Maker



- Nuff Said.

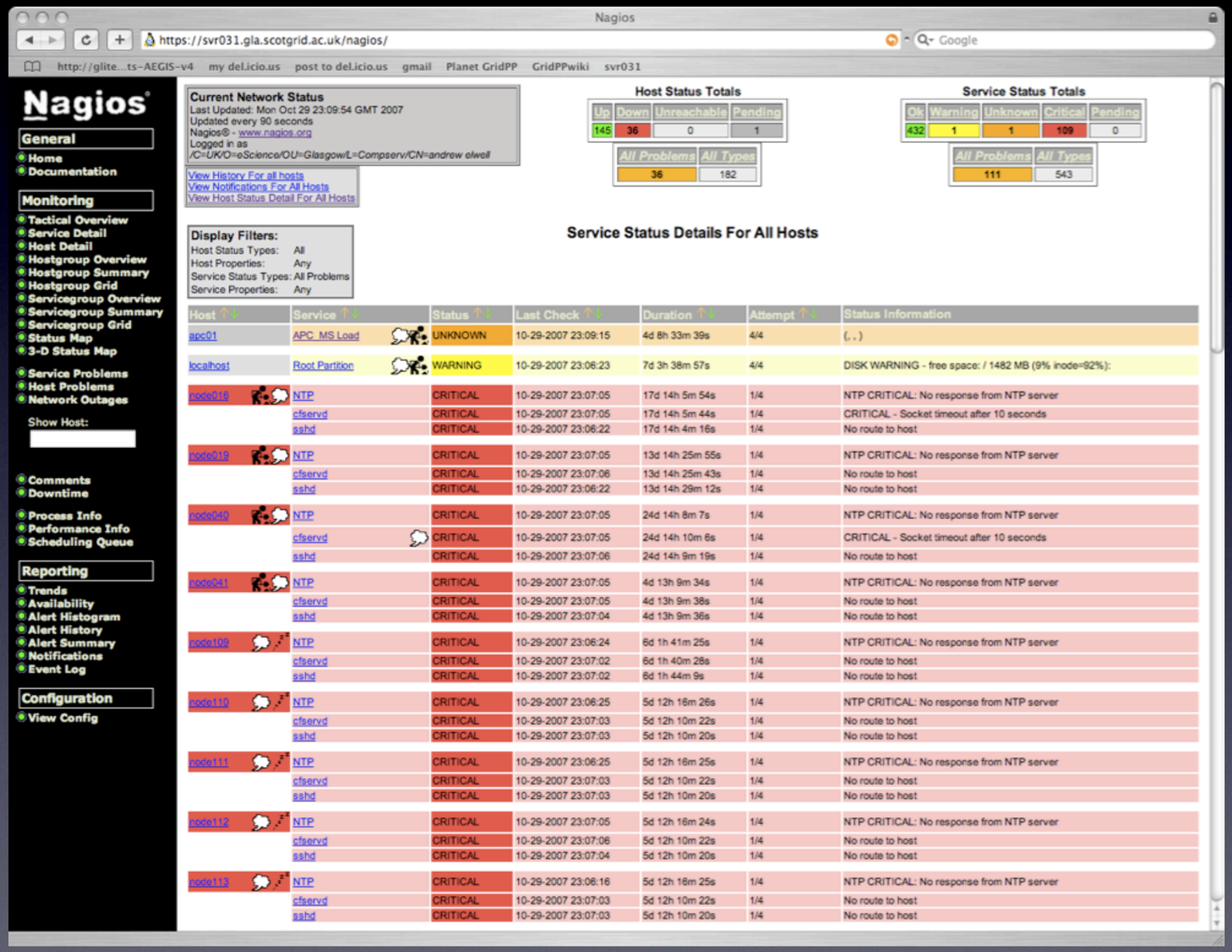
What is Nagios?

- "An Open Source host, service and network monitoring program"
- Central Daemon
  - intermittently polls hosts and services
  - uses plugins
  - returns the status information
  - Notifies / escalates depending on severity / pattern

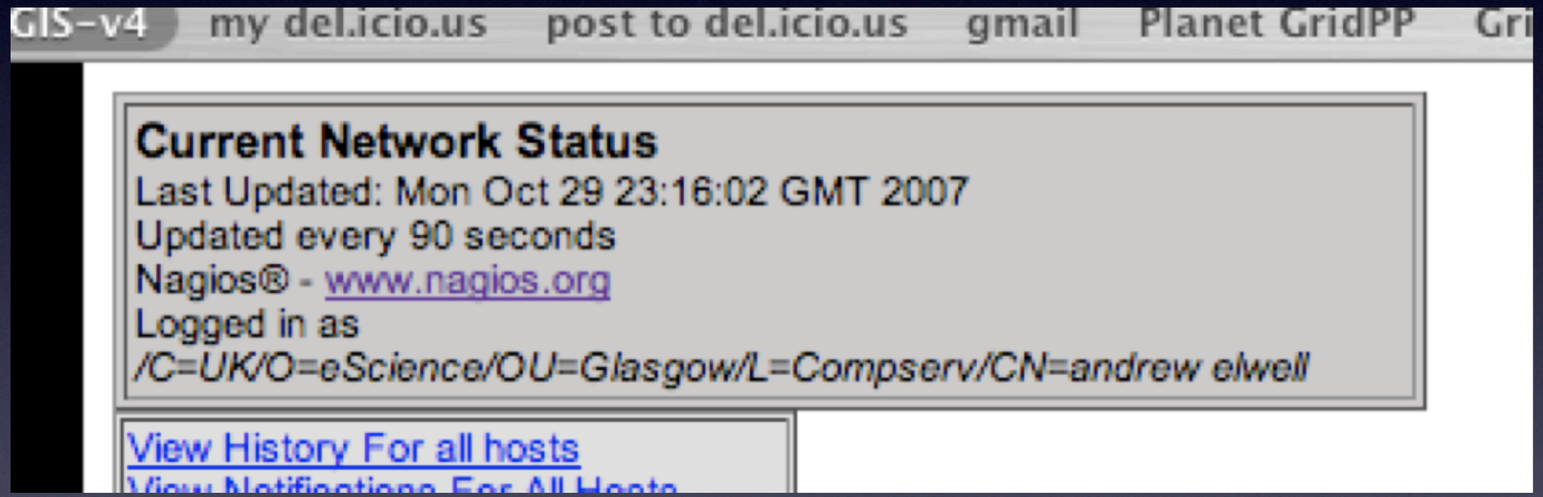
Nagios Overview

- http://www.nagios.org
- Ethan Galstad released under GPL2
- Version 2.10 (stable) and 3.0beta5
- Needs Linux and C compiler
- Web GUI - Apache and libgd
- Can also monitor Windows (NSClient) and Netware

Screenshots



Screenshots



Screenshots

Host Status Totals

Up	Down	Unreachable	Pending
145	36	0	1

All Problems	All Types
36	182

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
432	1	1	109	0

All Problems	All Types
111	543

Screenshots

Host	Service	Status	L
apc01	APC_MS Load	UNKNOWN	1
localhost	Root Partition	WARNING	1
node016	NTP	CRITICAL	1
	cfservd	CRITICAL	1
	sshd	CRITICAL	1
node019	NTP	CRITICAL	1
	cfservd	CRITICAL	1
	sshd	CRITICAL	1
node040	NTP	CRITICAL	1
	cfservd	CRITICAL	1
	sshd	CRITICAL	1
node041	NTP	CRITICAL	1
	cfservd	CRITICAL	1
	sshd	CRITICAL	1
node109	NTP	CRITICAL	1
	cfservd	CRITICAL	1
	sshd	CRITICAL	1
node110	NTP	CRITICAL	1
	cfservd	CRITICAL	1

Screenshots

[Uki-scotgrid-glasgow] ** PROBLEM alert - Worker Node 001/cfservd is CRITICA...

Delete Junk Reply Reply All Forward Print

From: nagios <nagios@svr031.gla.scotgrid.ac.uk>
Subject: **[Uki-scotgrid-glasgow] ** PROBLEM alert - Worker Node 001/cfservd is CRITICAL ****
Date: 30 October 2007 14:09:23 GMT
To: uki-scotgrid-glasgow@physics.gla.ac.uk

***** Nagios 2.7 *****

Notification Type: PROBLEM

Service: cfservd
Host: node001
Address: 10.141.0.1
State: CRITICAL

Date/Time: Tue Oct 30 14:09:23 GMT 2007

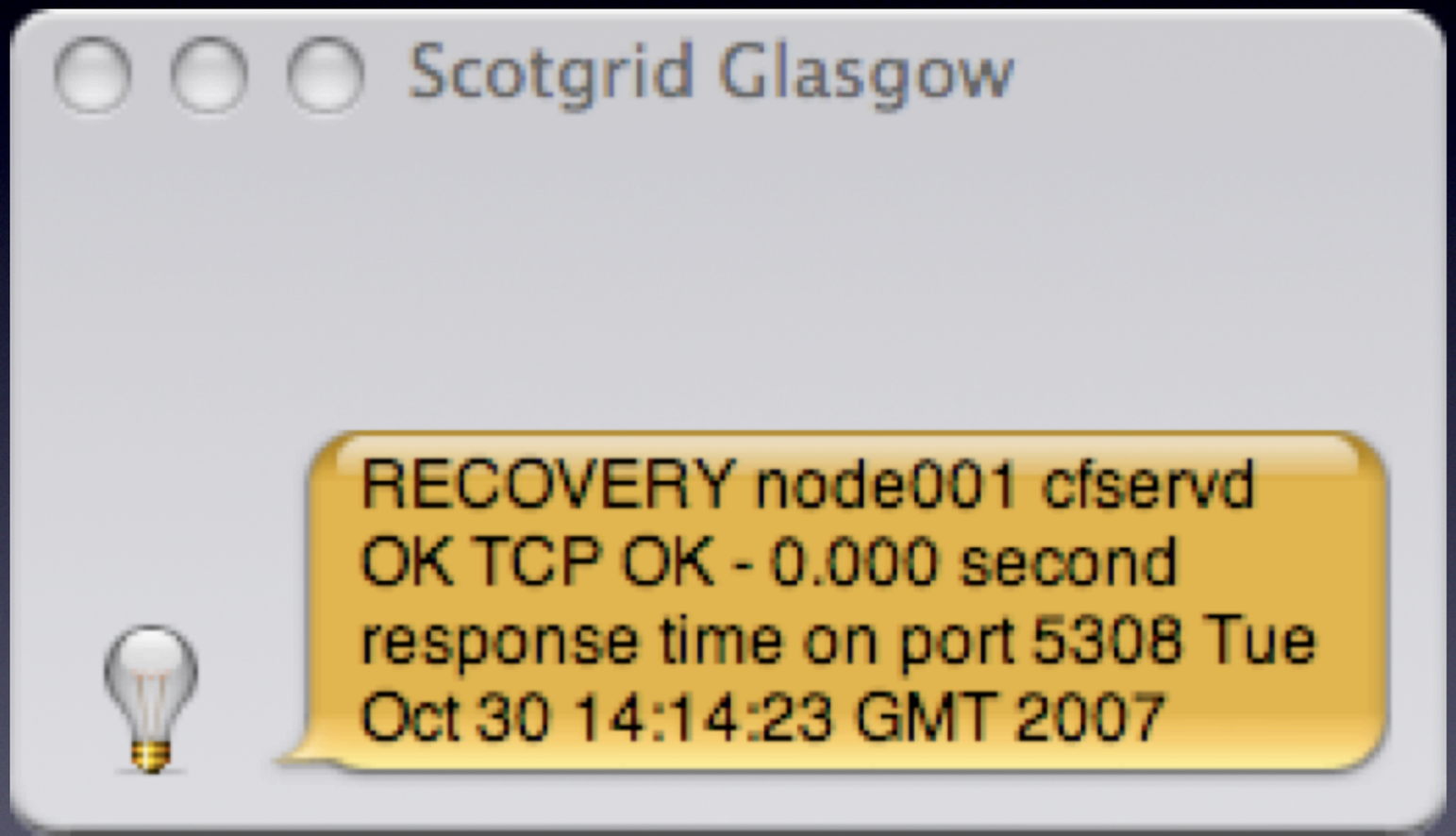
Additional Info:

Connection refused
Ack by:
Comments:

---

uki-scotgrid-glasgow mailing list
uki-scotgrid-glasgow@physics.gla.ac.uk
http://www.physics.gla.ac.uk/mailman/listinfo/uki-scotgrid-glasgow

Screenshots



Installation

- Choose a SECURE box to host it on that can see the network
- Source from nagios.org
- RPMs from DAG
  - nagios, nagios-plugins, nagios-plugins-nrpe, nagios-nsca
- .deb already in ubuntu (2.9)

Nagios Configuration Files

nagios.cfg
main config file that defines other files, logging, events etc.

Nagios Daemon

interprests files using macros defined in

resource.cfg
macros referred to in other files
e.g. $USER1$ = nagios home dir

refers to all other config files

refers to central configuration file

Apache

httpd.conf
apache include file describing how to display nagios web pages

points apache at cgi files secured by

.htaccess
apache security definition detailing allowed users

authenticates users defined in

htpasswd.users
people authorized to in parts of nagios and their passwords

cgi.cfg
parameters customizing the action of the web pages

authorizes users defined in

hostgroups.cfg
groups hosts into types for alerting and display purposes

have someone to complain to

contactgroups.cfg
contacts are grouped since we need some support redundancy

go to

escalations.cfg
if something breaks and is not fixed who can we complain to next

are grouped by type into

hosts.cfg
central monitoring component along with services

run on

are members of

are maintained by

contacts.cfg
people that we can call on to fix hosts and services

happen if unfixed breakage happens to

hosts may appear broken if other hosts break

dependencies.cfg
sometimes things wrongly appear dead because something else broke

are checked by

services.cfg
central monitoring component along with hosts

services may appear broken if other services break

will work the following hours

are notified by

timeperiods.cfg
for example "work hours" or "24 x 7" or "overtime"

function within

are checked by

misccommands.cfg
how to notify users that things are broken

checkcommands.cfg
how to check hosts and services are working

Configuration

- Start monitoring localhost until you get the basics
- Add in a new cfg_dir= into nagios.cfg
- Expand to ping test of your nodes
- Add a few network accessible services (sshd)
- Run probes on remote boxes

Config Tips

- check_period 24*7 even if notifications aren't
- Leave authentication up to Apache - use * in cgi.cfg
- See the 'Time Saving Tricks for Object Definitions' regexps and multiple hosts

Templates

```
cat <<EOF > $CFG
# Nagios config file for gla.scotgrid worker nodes
# built automatically from genhost.sh

define hostgroup{
        alias                   Worker Nodes
        hostgroup_name          workernodes
}

define host{
        name    wn_template
        use     linux-server
        hostgroups      workernodes
        register        0
}

define service{
        hostgroup_name  workernodes
        service_description sshd
        check_command   check_ssh
        servicegroups   sshservers
        use             local-service
}
EOF
```

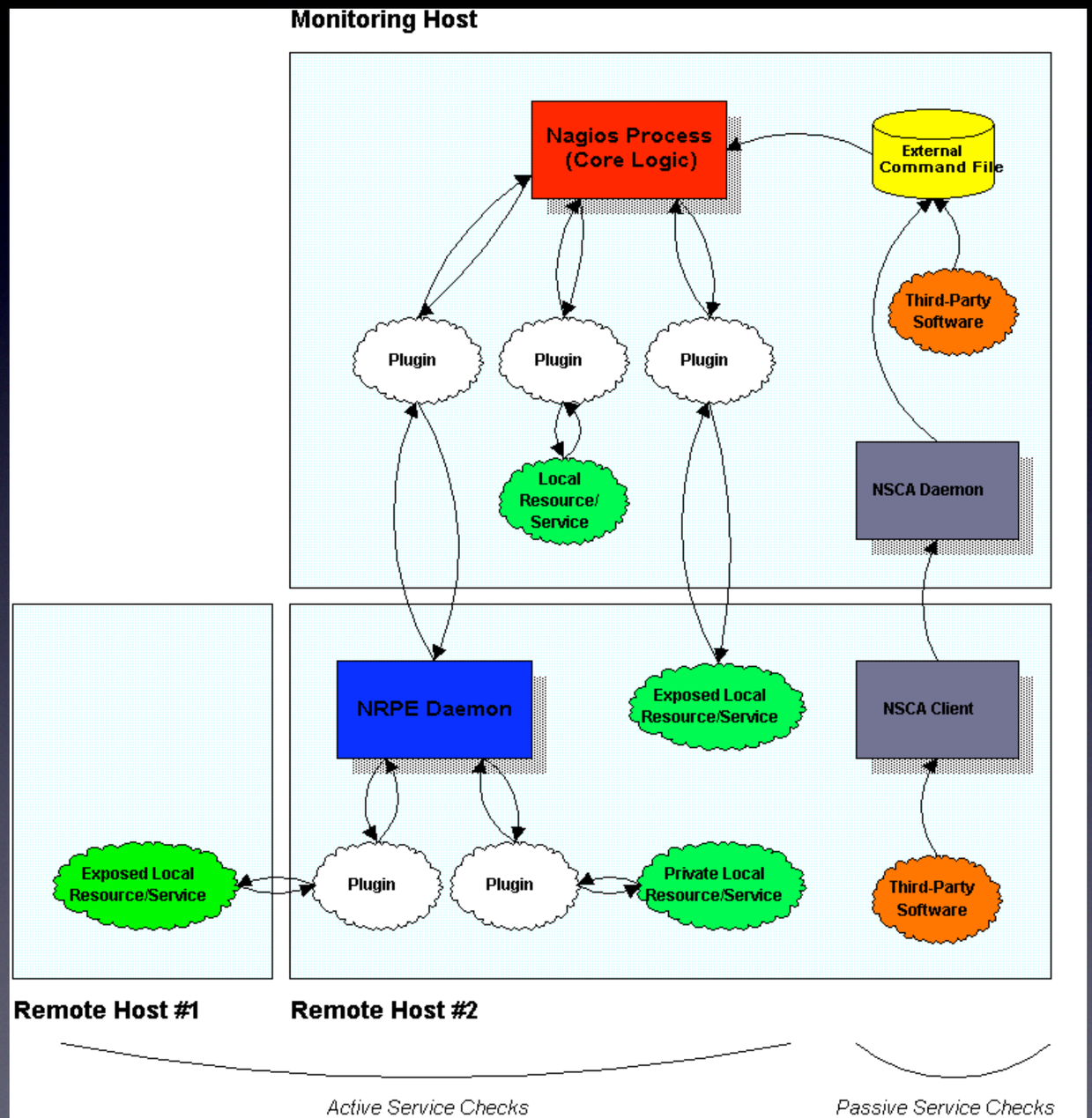
```
for i in `seq 1 140` ; do
h=`printf "%03d" $i`
cat <<EOF >> $CFG
define host {
        host_name       node$h
        alias           Worker Node $h
        address         10.141.0.$i
        use             wn_template
}

EOF
done
```

Plugins

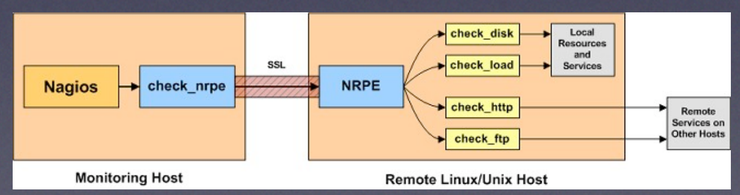
- Can be written in any language - exit code counts
- 0 - OK, 1 - Warning, 2 - Critical, 3 - Unknown
- http://nagiosplug.sf.net/developer-guidelines.html
- Plenty of included ones in the rpms
- Beware of overhead (switch to C / embPerl)

Active / Passive



NRPE

- Daemon runs on remote host (5666/tcp)
- Accepts SSL from check_nrpe
- Runs *previously defined* plugins on that host
- You need to install plugins on remote host...



NSCA

- Daemon runs on the nagios server
- Client spits output with send_nsca script
- Need to configure nagios to accept the passive checks
- <host_name>[tab]<svc_description>[tab]<return_code>[tab]<plugin_output>[newline]
- <host_name>[tab]<return_code>[tab]<plugin_output>[newline]

NSCA

- Daemon runs on the nagios server
- Client spits output with send_nsca script
- Need to configure nagios to accept the passive checks
- <host_name>[tab]<svc_description>[tab]<return_code>[tab]<plugin_output>[newline]
- <host_name>[tab]<return_code>[tab]<plugin_output>[newline]
- Yep, it works with MonAMI

Jabber / SMS

- Perl script that uses Net::XMPP
- Presently hacky as hard-coded @gmail.com address
- Edited contacts.cfg to include

```
...
pager andrew.elwell
service_notification_commands notify-by-jabber
host_notification_commands host-notify-by-jabber
service_notification_period 24x7
host_notification_period 24x7
...
```

Escalation

- Yep. Good Idea. We don't use it.

Event Handlers

- Attempts to fix critical services
- Log trouble tickets etc
- No, We don't use it...

Scheduled Maintenance

- stop nagios (blind)
- put node into maintenance using web page (single host)
- echo into the nagios pipe (scalable)

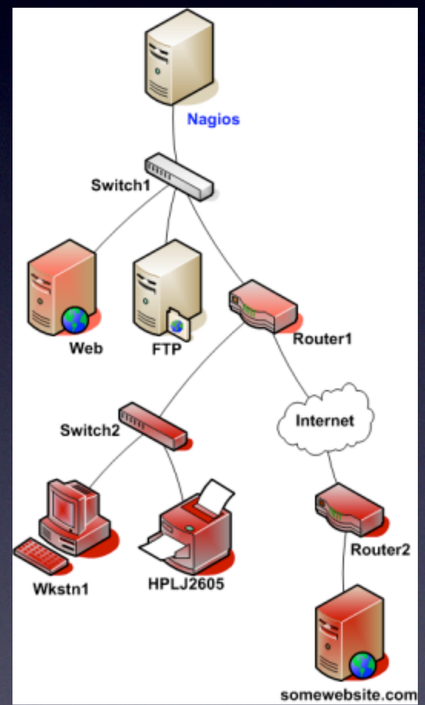
```
#!/bin/bash
# This is a sample shell script showing how you can submit the
SCHEDULE_HOST_DOWNTIME command
# to Nagios. Adjust variables to fit your environment as necessary.

now=`date +%s`
minus1h=$(($now - 3600))
plus1h=$(($now + 3600))
commandfile='/var/log/nagios/rw/nagios.cmd'
for i in `seq 109 138` 140 ; do
 /usr/bin/printf "[%lu] SCHEDULE_HOST_DOWNTIME;node$i;%lu;%lu;0;0;604800;
SysAdmins;Down to reduce power\n" \
      $now $minus1h $plus1h > $commandfile
done
```

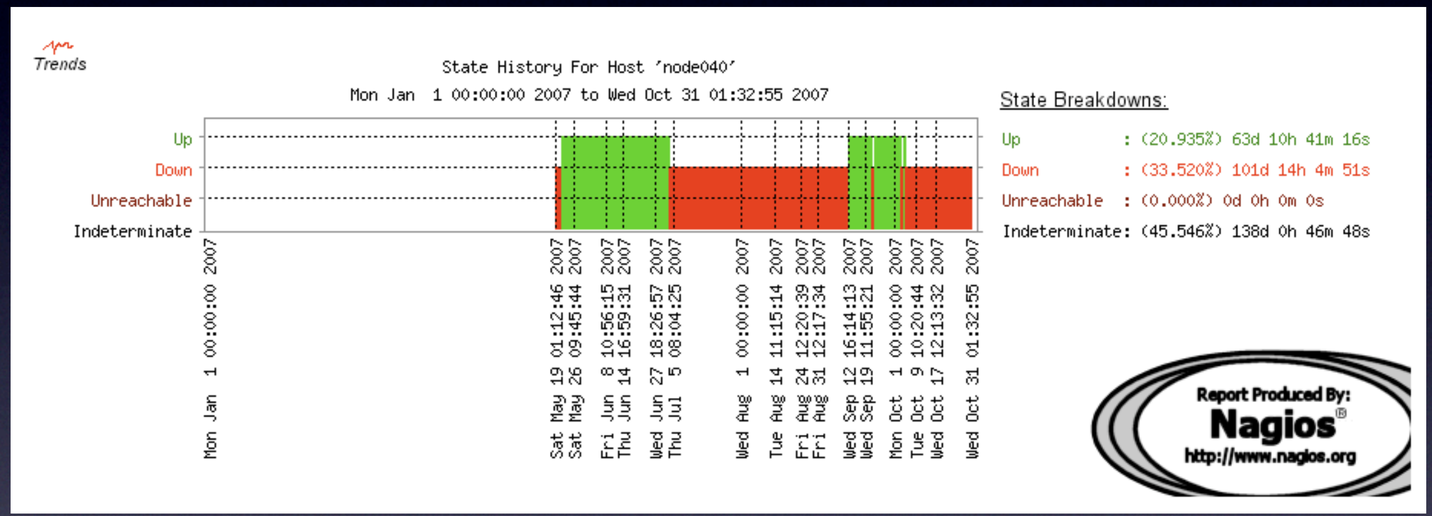
Dependencies

- DOWN
- UNREACHABLE

```
define host{
        host_name           Switch2
        parents             Router1
        }
```



Availability Reporting



More Info...

- Nagios Community Wiki - http://www.nagioscommunity.org/wiki/index.php/Main_Page
- Plugins http://nagiosplugins.org/
- Nagios Exchange http://www.nagiosexchange.org/
- http://www.gridpp.ac.uk/wiki/Nagios

snippets from 3.0 docs

- use_large_installation_tweaks - OS does memory cleanup, doesn't double fork() but no summary macros
- Multiline plugin output (from 350b to 4k)
- Docs are MUCH clearer than 2.0 ones
- Host checks run in parallel
- check_{host|service}_cluster for HA setups

Any Questions?